VIEDEV

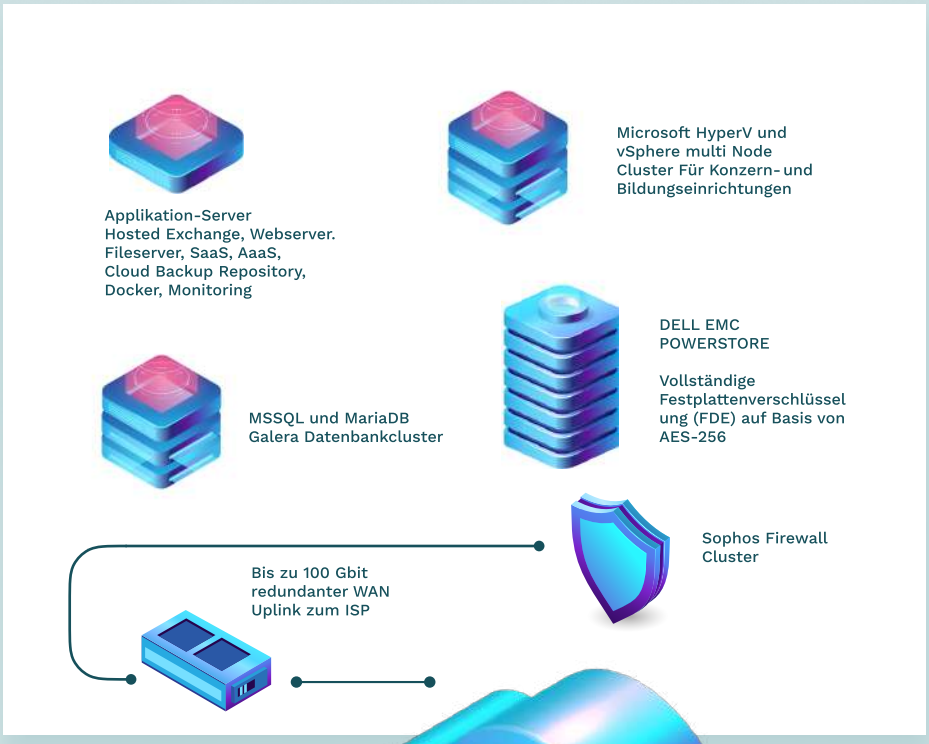
VIEDEV GmbH Rechenzentrums- und Sicherheitsbeschreibung

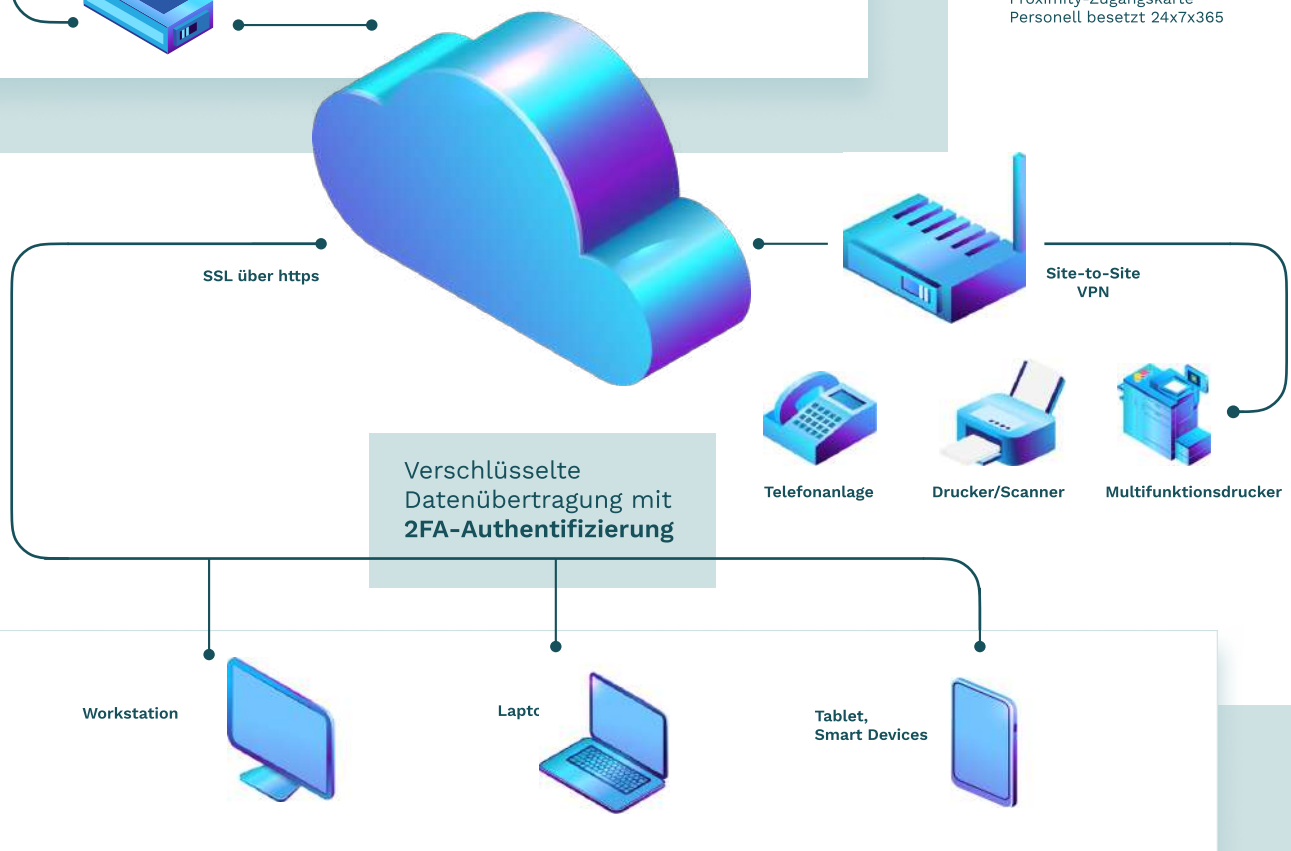
Stand Januar 2023

VIEDEV GmbH Rechenzentrums- und Sicherheitsbeschreibung

Stand Januar 2023

Rechenzentrum Frankfurt





RZ-Betreiber und VIEDEV-Partner:
BW-TECH GmbH
Albert-Bassermann-Straße 31
68782 Brühl

Träger:
Digital Reality
Lyoner Straße 28
60528 Frankfurt am Main

Gebäudedaten:
Gesamtfläche des Rechenzentrums: 4500 m²

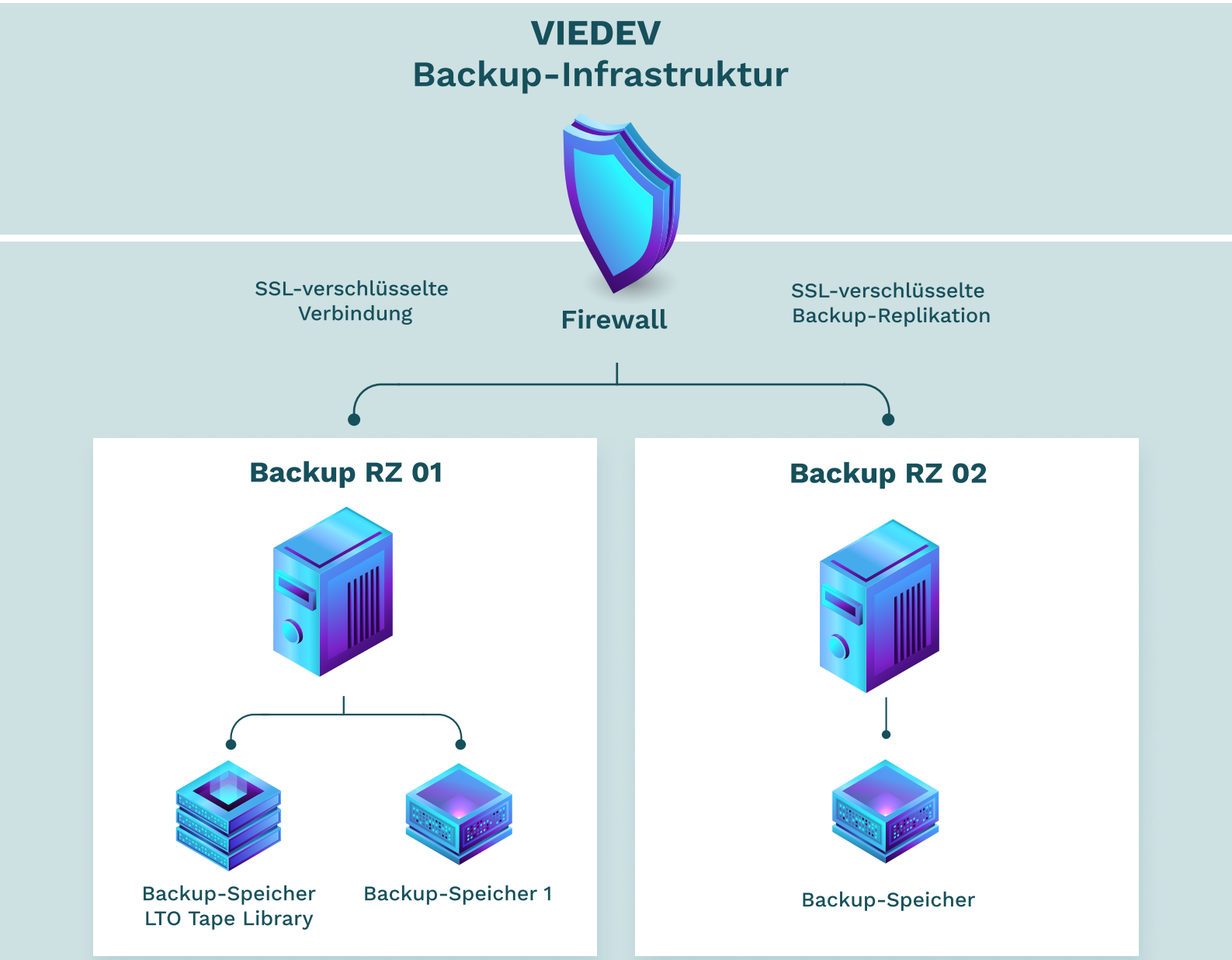
Speziell gebautes Datenzentrum:
Anzahl der Il-Zonen: 11
Hochwassergebiet: Nein
Erdbebengebiet: Nein
Stromversorgungskapazität: 19.8 MVA
USV-Leistungskapazität: 11.2 MVA
USV-Redundanz: N+l
Leistungsdichte: 1.24 kW/m
Generator-Leistungskapazität: 12 MVA
Kühlung Redundanz: N+l
Bodenbelastung: bis zu 1.500 kg/m²
Faser- und Gebäudezugang
Anzahl verschiedener Gebäudezugänge: 2
Anzahl der Meet-Me-Räume:
2 Trägerflächen

Sicherheitsmaßnahmen:
Proximity-Zugangskarte
Personell besetzt 24x7x365

VIEDEV GmbH Rechenzentrums- und Sicherheitsbeschreibung

Stand Januar 2023

VIEDEV Backup-Infrastruktur



RZ FRANKFURT

- entkoppelte eigenständige Backupdomain
- separate Passwortpolicies
- tägliche Kontrolle der gelaufenen Backups
- regelmäßige Restoretests der Backups
- individuelle Aufbewahrungszeiten gemäß Kundenwunsch möglich

RZ WIEN

- **verschlüsselte Ablage aller Backups**
- für Datenbankkunden ist die zusätzliche Backup-Replikation der Datenbanken für 30 Tage Aufbewahrungszeit inklusive
- auf Kundenwunsch können zusätzlich komplette Cloudserver an den zweiten Standort repliziert werden

Beschreibung der aktuellen Backup-Strategie:

- Es werden täglich zwischen 22:00 Uhr und 04:00 Uhr Snapshots-Backups mit der Datensicherungs-software Veeam durchgeführt. Datenbanken und Applikationen werden im konsistenten Zustand gesichert.
- Alle Datenbanken werden zusätzlich zwischen 07:00 Uhr und 22:00 Uhr wahlweise im 1-, 2- oder 3-Stunden-Takt gesichert.
- Die Backupserver stehen in einer eigenen Domain und einem eigenen Netzwerksegment. Ein direkter Zugriff aus der Terminal- bzw. Applikations-serverumgebung in die Backupumgebung ist nicht möglich.
- Der Backup- und der Produktivspeicher sind von unterschiedlicher Hardwaregeneration und nicht direkt miteinander verbunden.
- Es wird täglich eine zusätzliche Kopie vom Disk-Backupspeicher auf Magnetbänder angefertigt, die als „Offline“-Technologie nicht von Ransomware angegriffen werden kann.
- Datenbanken sind im Regelfall auf separaten Systemen untergebracht und es besteht keine direkte Dateisystemverbindung zum Applikationsserver.
- Um unseren Kunden einen erweiterten Randsomwareschutz anzubieten, wurde ab Oktober 2021 eine zusätzliche, tägliche und verschlüsselte Replikation der Datenbanksicherungen in unser zweites RZ in Wien eingerichtet.
- Ebenfalls besteht ab Oktober 2021 die Möglichkeit für Cloudkunden, die kompletten Systeme mit individueller Aufbewahrungszeit in unser zweites RZ zu replizieren.

Beschreibung des aktuellen Virenschutzes:

- Alle Systeme sind zusätzlich mit der Sophos Live Protection ausgestattet.
- Sophos Endpoint Security and Control ist eine integrierte Suite von Sicherheitssoftware.
- Sophos Anti-Virus erkennt und bereinigt Viren, Trojaner, Würmer und Spyware sowie Adware und andere potenziell unerwünschte Anwendungen. Die eingesetzte HIPS-Technologie (Host Intrusion Prevention System) kann Ihren Computer auch vor verdächtigen Dateien und Rootkits schützen. Darüber hinaus kann Malicious Traffic Detector die Kommuni-kation zwischen Ihrem Computer und Befehls- und Steuerservern erkennen, die an einem Botnet- oder anderen Malware-Angriff beteiligt sind.
- Der Sophos Virenscanner ist dauerhaft aktiv und kann nicht vom Endkunden beendet werden. Wöchentlich wird ein geplanter Full Scan der VM durchgeführt. Der aktive Zugriffscan bei Zugriff auf Dateien ist standardmäßig aktiviert.

Beschreibung der aktuellen Firewall:

- Als hochverfügbares Firewall Cluster kommt eine Sophos-UTM-Firewall-Lösung zum Einsatz. Jede virtuelle Maschine befindet sich in einem /30-Subnetz und einem separaten VLAN. Da die Kommunikation über die Sophos Firewall aktiv geroutet werden muss, ist hier ein Paket-Filter aktiv. Die Kommunikation zwischen Endkunden-Systemen ist im Regelwerk der Firewall nicht erlaubt.
- Sollte ein Kunde spezielle Applikationen betreiben, die zusätzliche freigegebene Ports benötigen, ist dies unter Berücksichtigung einer vorherigen Sicherheitsprüfung möglich.
- Zugriff zum kundeneigenen VLAN ist nur mit einer vom Rechenzentrum gestellten VPN, site-to-site oder einer verschlüsselten RAS Verbindung möglich. Die Zugriffe werden von der Firewall überwacht um unerwünschten Traffic auszuschließen.

Zertifizierungen Rechenzentrum FRA / VIE*

- ISO 9001 - FRA/VIE
- ISO 14001 - FRA
- ISO 27001 - FRA/VIE
- ISO 50001 - FRA/VIE
- OHSAS 18001 - FRA
- ISAE 3402 Type II - VIE
- Tier 3-TIA 942/G - VIE
- ISO 50600 - VIE
- PCI DSS - VIE

Support, Service & Dienstleistung:

Kunden mit einem gültigen Supportvertrag und deren zertifizierte Supportpartner können eine der folgenden Möglichkeiten nutzen, um den **VIEDEV-Support** zu kontaktieren:

support@viedev.com **+49 (0)8022 / 8646010** **Mo.- Fr. 09:00 - 17:00**

Servicevereinbarung* & Verfügbarkeit:

• **Evaluierung und Installationsunterstützung:**	Mo.- Fr. 9 bis 17 Uhr E-Mail und Support-Hotline
• **Entry, Standard, Advanced Support:**	Mo.- Fr. 9 bis 17 Uhr E-Mail und Support-Hotline
• **Premium Support:**	Mo.- Fr. 8 bis 20 Uhr E-Mail und Support-Hotline
• **Enterprise Support:**	**24/7** E-Mail und Support-Hotline
• **Emergency:**	**24/7** Support-Hotline

VIEDEV